Konfigurieren

ONTAP 9

NetApp
April 13, 2024

Inhalt

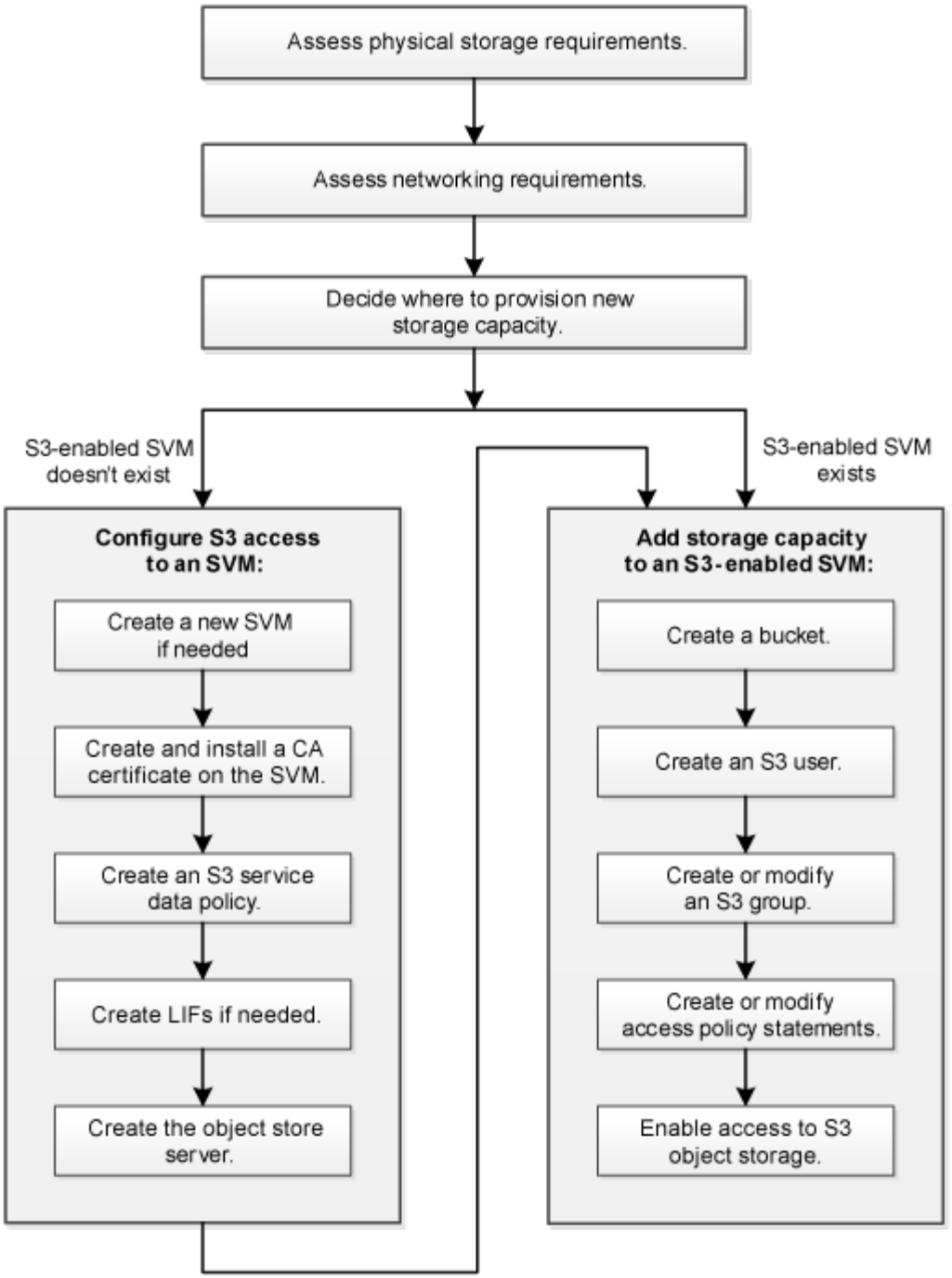
Konfigurieren

Allgemeines zur S3-Konfiguration

S3-Konfigurationsworkflow

Bei der Konfiguration von S3 geht es darum, physische Storage- und Netzwerkanforderungen zu bewerten, und anschließend einen spezifischen Workflow auszuwählen: S3-Zugriff auf eine neue oder vorhandene SVM zu konfigurieren oder einen Bucket und Benutzer zu einer vorhandenen SVM hinzuzufügen, die bereits vollständig für S3-Zugriff konfiguriert ist.

Wenn Sie mit System Manager S3-Zugriff auf eine neue Storage-VM konfigurieren, müssen Sie Zertifikat- und Netzwerkinformationen eingeben. Die Storage-VM und der S3-Objekt-Storage-Server werden in einem Vorgang erstellt.



Physischer Storage-Bedarf bewerten

Bevor Sie S3-Storage für die Clients bereitstellen, müssen Sie sicherstellen, dass in vorhandenen Aggregaten für den neuen Objektspeicher ausreichend Speicherplatz vorhanden ist. Wird dies nicht der Fall sein, können Sie den gewünschten Typ und den gewünschten Speicherort mit Festplatten zu vorhandenen Aggregaten hinzufügen oder neue Aggregate erstellen.

Über diese Aufgabe

Wenn Sie einen S3-Bucket in einer S3-fähigen SVM erstellen, wird automatisch ein FlexGroup-Volume erstellt, um den Bucket zu unterstützen. Sie können ONTAP Select die zugrunde liegenden Aggregate und FlexGroup

Komponenten automatisch (das Standard) lassen oder Sie können die zugrunde liegenden Aggregate und FlexGroup Komponenten selbst auswählen.

Wenn Sie sich entscheiden, die Aggregate und FlexGroup-Komponenten anzugeben, z. B. wenn Sie bestimmte Performance-Anforderungen für die zugrunde liegenden Festplatten haben — sollten Sie sicherstellen, dass die Aggregatkonfiguration den Best Practice-Richtlinien für die Bereitstellung eines FlexGroup Volume entspricht. Weitere Informationen:

- "Management von FlexGroup Volumes"
- "Technischer Bericht 4571-a: NetApp ONTAP FlexGroup Volume Top Best Practices"

Wenn Sie Buckets von Cloud Volumes ONTAP bereitstellen, wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Node verwenden. Die Verwendung von Aggregaten beider Nodes kann sich auf die Performance auswirken, da die Nodes sich in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind. Erfahren Sie mehr über "Erstellen von Buckets für Cloud Volumes ONTAP".

Sie können den ONTAP S3-Server verwenden, um eine lokale FabricPool-Kapazitäts-Tier zu erstellen, d. h. im selben Cluster wie die Performance-Tier. Dies kann beispielsweise nützlich sein, wenn Sie SSD-Festplatten an ein HA-Paar angeschlossen haben und Sie *Cold* Daten auf HDD-Festplatten in einem anderen HA-Paar verschieben möchten. In diesem Anwendungsfall sollten sich der S3-Server und der Bucket, der die lokale Kapazitäts-Tier enthält, daher in einem anderen HA-Paar als das Performance-Tier befinden. Lokales Tiering wird nicht auf Clustern mit einem oder zwei Nodes unterstützt.

Schritte

1. Anzeige des verfügbaren Speicherplatzes in vorhandenen Aggregaten:

   ```
   storage aggregate show
   ```

   Wenn genügend Speicherplatz oder der erforderliche Speicherort für ein Aggregat vorhanden ist, notieren Sie seinen Namen für die S3-Konfiguration.

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. Falls keine Aggregate genügend Speicherplatz oder den erforderlichen Node-Standort vorhanden sind, fügen Sie mithilfe der Festplatten zu einem vorhandenen Aggregat hinzu `storage aggregate add-disks` Befehl, oder erstellen Sie mit dem ein neues Aggregat `storage aggregate create` Befehl.

Netzwerkanforderungen bewerten

Bevor Sie Clients S3 Storage bereitstellen, müssen Sie überprüfen, ob Netzwerke korrekt konfiguriert sind, um die S3-Bereitstellungsanforderungen zu erfüllen.

Bevor Sie beginnen

Die folgenden Cluster-Netzwerkobjekte müssen konfiguriert werden:

- Physische und logische Ports
- Broadcast-Domänen
- Subnetze (falls erforderlich)
- IPspaces (nach Bedarf zusätzlich zum Standard-IPspace)
- Failover-Gruppen (falls erforderlich, zusätzlich zur Standard-Failover-Gruppe für jede Broadcast-Domäne)
- Externe Firewalls

Über diese Aufgabe

Für Cloud-Tiers (Remote FabricPool Capacity) und Remote-S3-Clients müssen Sie eine Daten-SVM verwenden und Daten-LIFs konfigurieren. Für FabricPool Cloud Tiers müssen Sie außerdem Intercluster LIFs konfigurieren, Cluster-Peering ist nicht erforderlich.

Für lokale FabricPool-Kapazitäts-Tiers müssen Sie die System-SVM (namens „`Cluster`“) verwenden, aber es gibt zwei Optionen für die LIF-Konfiguration:

- Sie können die Cluster-LIFs verwenden.

  Bei dieser Option ist keine weitere LIF-Konfiguration erforderlich, doch der Datenverkehr auf Cluster-LIFs wird erhöht. Außerdem kann andere Cluster nicht auf die lokale Tier zugreifen.

- Sie können Daten verwenden und LIFs Intercluster verwenden.

  Diese Option erfordert eine zusätzliche Konfiguration, einschließlich der Aktivierung der LIFs für das S3-Protokoll, aber auf die lokale Tier kann auch für andere Cluster als Remote-FabricPool-Cloud-Tier zugegriffen werden.

Schritte

1. Anzeigen der verfügbaren physischen und virtuellen Ports:

   ```
   network port show
   ```

   - Wenn möglich, sollten Sie den Port mit der höchsten Geschwindigkeit für das Datennetzwerk verwenden.
   - Für optimale Performance müssen alle Komponenten im Datennetzwerk dieselbe MTU-Einstellung aufweisen.

2. Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, überprüfen Sie, ob das Subnetz existiert und über ausreichende Adressen verfügbar ist:

```
network subnet show
```

Subnetze enthalten einen Pool mit IP-Adressen, die zum selben Layer-3-Subnetz gehören. Subnetze werden mithilfe des erstellt `network subnet create` Befehl.

3. Verfügbare IPspaces anzeigen:

```
network ipspace show
```

Sie können den Standard-IPspace oder einen benutzerdefinierten IPspace verwenden.

4. Wenn Sie IPv6-Adressen verwenden möchten, überprüfen Sie, ob IPv6 auf dem Cluster aktiviert ist:

```
network options ipv6 show
```

Bei Bedarf können Sie IPv6 mithilfe des aktivieren `network options ipv6 modify` Befehl.

Legen Sie fest, wo neue S3-Storage-Kapazität bereitgestellt werden soll

Bevor Sie einen neuen S3-Bucket erstellen, müssen Sie entscheiden, ob er in eine neue oder vorhandene SVM platziert werden soll. Diese Entscheidung bestimmt Ihren Workflow.

Wahlmöglichkeiten

- Wenn Sie einen Bucket in einer neuen SVM oder einer SVM bereitstellen möchten, der für S3 nicht aktiviert ist, führen Sie die Schritte in den folgenden Themen aus.

  "Erstellung einer SVM für S3"

  "Erstellen eines Buckets für S3"

  Obwohl S3 parallel in einer SVM mit NFS und SMB eingesetzt werden kann, können Sie möglicherweise eine neue SVM erstellen, sofern eine der folgenden Optionen zutrifft:

  - Sie aktivieren erstmals S3 auf einem Cluster.
  - Sie verfügen über vorhandene SVMs in einem Cluster, in dem die S3-Unterstützung nicht aktiviert werden soll.
  - Sie verfügen über eine oder mehrere S3-fähige-SVMs in einem Cluster und möchten einen weiteren S3-Server mit unterschiedlichen Performance-Merkmalen nutzen. Nachdem Sie S3 auf der SVM aktiviert haben, fahren Sie mit der Bereitstellung eines Buckets fort.

- Wenn Sie den anfänglichen Bucket oder einen zusätzlichen Bucket auf einer vorhandenen S3-fähigen SVM bereitstellen möchten, führen Sie die Schritte im folgenden Thema aus.

  "Erstellen eines Buckets für S3"

Konfigurieren des S3-Zugriffs auf eine SVM

Erstellung einer SVM für S3

Obwohl S3 parallel zu anderen Protokollen in einer SVM unterstützt werden kann, sollten

Sie möglicherweise eine neue SVM erstellen, um Namespace und Workload zu isolieren.

Über diese Aufgabe

Wenn Sie lediglich S3-Objekt-Storage über eine SVM bereitstellen, ist für den S3-Server keine DNS-Konfiguration erforderlich. Allerdings möchten Sie DNS möglicherweise auf der SVM konfigurieren, wenn andere Protokolle verwendet werden.

Wenn Sie mit System Manager S3-Zugriff auf eine neue Storage-VM konfigurieren, müssen Sie Zertifikat- und Netzwerkinformationen eingeben. Die Storage-VM und der S3-Objekt-Storage-Server werden in einem Vorgang erstellt.

Beispiel 1. Schritte

System Manager

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den die Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

Sie sollten darauf vorbereitet sein, IP-Adressen für die Schnittstellenrollendaten einzugeben.

Wenn Sie ein von einer externen Zertifizierungsstelle signiertes Zertifikat verwenden, werden Sie aufgefordert, es während dieses Verfahrens einzugeben. Sie haben auch die Möglichkeit, ein vom System generiertes Zertifikat zu verwenden.

1. Aktivieren Sie S3 auf einer Storage-VM.

   a. Fügen Sie eine neue Speicher-VM hinzu: Klicken Sie auf **Storage > Storage VMs** und dann auf **Hinzufügen**.

      Falls es sich um ein neues System ohne bereits vorhandene Storage-VMs handelt, klicken Sie auf **Dashboard > Protokolle konfigurieren**.

   Wenn Sie einen S3-Server zu einer vorhandenen Speicher-VM hinzufügen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann auf Unter **S3**.

   a. Klicken Sie auf **S3** aktivieren und geben Sie dann den S3-Servernamen ein.

   b. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.

   c. Geben Sie die Netzwerkschnittstellen ein.

2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   - Der Geheimschlüssel wird nicht mehr angezeigt.
   - Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Vergewissern Sie sich, dass S3 für Ihr Cluster lizenziert ist:

   ```
   system license show -package s3
   ```

   Falls nicht, wenden Sie sich an Ihren Vertriebsmitarbeiter.

2. SVM erstellen:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- Verwenden Sie die UNIX-Einstellung für den `-rootvolume-security-style` Option.
- Verwenden Sie die Standard-C.UTF-8 `-language` Option.
- Der `ipspace` Die Einstellung ist optional.

3. Konfiguration und Status der neu erstellten SVM überprüfen:

```
vserver show -vserver <svm_name>
```

Der `Vserver Operational State` Das Feld muss angezeigt werden `running` Bundesland. Wenn der angezeigt wird `initializing` Zustand: Einiger Zwischenvorgang wie z. B. die Erstellung des Root-Volumes ist fehlgeschlagen. Außerdem müssen Sie die SVM löschen und erneut erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace ipspace A erstellt:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde und dass sie automatisch gestartet wurde und sich in befindet `running` Bundesland. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird. Standardmäßig wird das vsadmin-Benutzerkonto erstellt und befindet sich in `locked` Bundesland. Die vsadmin-Rolle ist dem vsadmin-Standardbenutzerkonto zugewiesen.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Erstellen und installieren Sie ein CA-Zertifikat auf der SVM

Um den HTTPS-Datenverkehr von S3-Clients auf die S3-fähige SVM zu aktivieren, ist ein CA-Zertifikat erforderlich.

Über diese Aufgabe

Zwar ist es möglich, einen S3-Server so zu konfigurieren, dass nur HTTP verwendet wird. Clients können zwar auch ohne CA-Zertifikat konfiguriert werden, es empfiehlt sich jedoch, den HTTPS-Datenverkehr auf ONTAP S3-Servern mit einem CA-Zertifikat zu sichern.

Ein CA-Zertifikat ist nicht erforderlich für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Traffic nur über die Cluster LIFs erfolgt.

Die Anweisungen in diesem Verfahren erstellen und installieren ein selbstsigniertes ONTAP-Zertifikat. CA-Zertifikate von Drittanbietern werden ebenfalls unterstützt. Weitere Informationen finden Sie in der Dokumentation zur Administratorauthentifizierung.

"Administratorauthentifizierung und RBAC"

Siehe `security certificate` Man-Pages für weitere Konfigurationsoptionen.

Schritte

1. Erstellen eines selbstsignierten digitalen Zertifikats:

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   Der `-type root-ca` Option erstellt und installiert ein selbstsigniertes digitales Zertifikat, um andere Zertifikate zu signieren, indem es als Zertifizierungsstelle fungiert.

   Der `-common-name` Option erstellt den Namen der Zertifizierungsstelle (CA) der SVM und wird verwendet, wenn der vollständige Name des Zertifikats generiert wird.

   Die standardmäßige Zertifikatsgröße beträgt 2048 Bit.

   Beispiel

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Wenn der generierte Name des Zertifikats angezeigt wird, speichern Sie ihn für die nachfolgenden Schritte.

2. Erzeugen einer Anfrage zum Signieren eines Zertifikats:

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   Der `-common-name` Der Parameter für die Signaturanforderung muss der S3-Servername (FQDN) sein.

   Gegebenenfalls können Sie den Speicherort und weitere detaillierte Informationen zur SVM angeben.

   Sie werden aufgefordert, eine Kopie Ihrer Zertifikatsanfrage und einen privaten Schlüssel für zukünftige Referenz aufzubewahren.

3. Signieren Sie die CSR mit SVM_CA, um das S3-Server-Zertifikat zu generieren:

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   Geben Sie die Befehlsoptionen ein, die Sie in früheren Schritten verwendet haben:

   - `-ca` — der allgemeine Name der CA, die Sie in Schritt 1 eingegeben haben.
   - `-ca-serial` — die CA-Seriennummer von Schritt 1. Wenn der Name des CA-Zertifikats beispielsweise svm1_ca_159D1587CE21E9D4_svm1_ca lautet, lautet die Seriennummer 159D1587CE21E9D4.

     Standardmäßig läuft das signierte Zertifikat in 365 Tagen ab. Sie können einen anderen Wert auswählen und weitere Signierungsdetails angeben.

Wenn Sie dazu aufgefordert werden, kopieren Sie die Zeichenfolge für die Zertifikatanforderung, die Sie in Schritt 2 gespeichert haben, und geben Sie sie ein.

Es wird ein signiertes Zertifikat angezeigt und zur späteren Verwendung gespeichert.

4. Installieren Sie das signierte Zertifikat auf der S3-fähigen SVM:

   `security certificate install -type server -vserver svm_name`

   Geben Sie bei Aufforderung das Zertifikat und den privaten Schlüssel ein.

   Sie haben die Möglichkeit, Zwischenzertifikate einzugeben, wenn eine Zertifikatkette gewünscht wird.

   Wenn der private Schlüssel und das CA-signierte digitale Zertifikat angezeigt werden, speichern Sie sie für zukünftige Referenz.

5. Holen Sie sich das Zertifikat für den öffentlichen Schlüssel:

   `security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

   Speichern Sie das Zertifikat für den öffentlichen Schlüssel für eine spätere Client-seitige Konfiguration.

   Beispiel

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
          FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
               Certificate Authority: svm1_ca
                 Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
             Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
              Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
             Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Erstellen einer S3-Service-Datenrichtlinie

Es können Service-Richtlinien für S3-Daten und Managementservices erstellt werden. Für die Aktivierung des S3-Datenverkehrs auf LIFs ist eine S3-Service-Datenrichtlinie erforderlich.

Über diese Aufgabe

Eine Datenrichtlinie für den S3-Service ist erforderlich, wenn Sie Daten-LIFs und Intercluster-LIFs verwenden. Wenn Sie Cluster-LIFs für den lokalen Tiering-Anwendungsfall verwenden, ist dies nicht erforderlich.

Wenn eine Service-Richtlinie für eine LIF angegeben wird, wird diese Richtlinie verwendet, um eine Standardrolle, Failover-Richtlinie und Datenprotokollliste für die LIF zu erstellen.

Obwohl mehrere Protokolle für SVMs und LIFs konfiguriert werden können, empfiehlt es sich, S3 als einziges Protokoll für die Bereitstellung von Objektdaten zu verwenden.

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Service-Datenrichtlinie erstellen:

```
network interface service-policy create -vserver svm_name -policy policy_name
-services data-core,data-s3-server
```

Der `data-core` Und `data-s3-server` Services sind die einzigen erforderlich, die für die Aktivierung von ONTAP S3 erforderlich sind, andere Services können jedoch bei Bedarf eingebunden werden.

Erstellung von Daten-LIFs

Wenn Sie eine neue SVM erstellt haben, sollten die dedizierten LIFs, die Sie für S3-Zugriff erstellen, Daten-LIFs sein.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerk-Port muss für den Administrator konfiguriert worden sein `up` Status:
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

  Subnetze enthalten einen Pool mit IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem erstellt `network subnet create` Befehl.

- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie eine große Anzahl von LIFs im Cluster besitzen, können Sie die im Cluster unterstützte LIF-Kapazität mithilfe der überprüfen `network interface capacity show` Befehl und die LIF-Kapazität, die auf jedem Node mithilfe von unterstützt wird `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene).
- Wenn Sie das Cloud-Tiering (Remote FabricPool Capacity) aktivieren, müssen Sie auch LIFs für Intercluster konfigurieren.

Schritte

1. LIF erstellen:

```
network interface create -vserver svm_name -lif lif_name -service-policy
service_policy_names -home-node node_name -home-port port_name {-address
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
data -auto-revert {true|false}
```

   - `-home-node` Ist der Node, den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.

     Sie können auch angeben, ob die LIF automatisch auf den Home-Node und den Home-Port mit zurückgesetzt werden soll `-auto-revert` Option.

   - `-home-port` Ist der physische oder logische Port, an den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.

- Sie können eine IP-Adresse mit dem angeben `-address` Und `-netmask` Optionen, oder Sie aktivieren die Zuweisung von einem Subnetz mit dem `-subnet_name` Option.
- Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
- Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Der `network route create` Die man-Page enthält Informationen zum Erstellen einer statischen Route in einer SVM.
- Für das `-firewall-policy` Wählen Sie die gleiche Standardeinstellung aus `data` Die LIF-Rolle.

  Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

  > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

- `-auto-revert` Ermöglicht Ihnen, anzugeben, ob eine Daten-LIF automatisch auf den Home-Node zurückgesetzt wird. Dies kann unter Umständen wie „Startvorgang“, ändert den Status der Management-Datenbank oder wenn die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Aber Sie können es auf einstellen `false` Abhängig von Netzwerkmanagement-Richtlinien in Ihrer Umgebung.
- Der `-service-policy` Option gibt die von Ihnen erstellte Daten- und Management-Services-Richtlinie sowie alle weiteren Richtlinien an, die Sie benötigen.

2. Wenn Sie im eine IPv6-Adresse zuweisen möchten `-address` Option:

   a. Verwenden Sie die `network ndp prefix show` Befehl zum Anzeigen der Liste der RA-Präfixe, die auf verschiedenen Schnittstellen gelernt wurden.

      Der `network ndp prefix show` Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

   b. Verwenden Sie das Format `prefix:id` Um die IPv6-Adresse manuell zu erstellen.

      `prefix` Ist das Präfix auf verschiedenen Schnittstellen gelernt.

   Für die Ableitung der `id`, Wählen Sie eine zufällige 64-Bit-Hexadezimalzahl aus.

3. Überprüfen Sie, ob das LIF erfolgreich mit dem erstellt wurde `network interface show` Befehl.
4. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Mit dem folgenden Befehl wird gezeigt, wie eine S3-Daten-LIF erstellt wird, die dem zugewiesen ist `my-S3-`

`policy` Service-Richtlinie:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird mit einer IPv6-Adresse konfiguriert:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Erstellen von Intercluster LIFs für Remote FabricPool Tiering

Wenn Sie Cloud-Tiering (Remote FabricPool Capacity) mit ONTAP S3 aktivieren, müssen Sie Intercluster LIFs konfigurieren. Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerk-Port muss für den Administrator konfiguriert worden sein `up` Status:
- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.

Über diese Aufgabe

Intercluster LIFs sind für das lokale Fabric Pool Tiering oder für die Bereitstellung externer S3-Applikationen nicht erforderlich.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Im folgenden Beispiel werden die Netzwerkports in angezeigt `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

   `network interface create -vserver Cluster -lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

   Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

   `network interface show –service-policy default-intercluster -failover`

   Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf dem `e0c` Ein Failover des Ports zum erfolgt `e0d` Port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Erstellen Sie den S3-Objektspeicher-Server

Der ONTAP Objektspeicher-Server managt Daten als S3-Objekte, anstatt von Datei- oder Block-Storage, der von ONTAP NAS- und SAN-Servern bereitgestellt wird.

Bevor Sie beginnen

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den die Clients für den S3-Zugriff verwenden. Der FQDN darf nicht mit einem Bucket-Namen beginnen.

Sie sollten über ein selbstsigniertes CA-Zertifikat (erstellt in vorherigen Schritten) oder ein Zertifikat, das von einem externen CA-Anbieter signiert wurde. Ein CA-Zertifikat ist nicht erforderlich für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Traffic nur über die Cluster LIFs erfolgt.

Über diese Aufgabe

Wenn ein Objektspeicher-Server erstellt wird, wird ein Root-Benutzer mit UID 0 erstellt. Für diesen Root-Benutzer wird kein Zugriffsschlüssel oder geheimer Schlüssel generiert. Der ONTAP-Administrator muss den ausführen `object-store-server users regenerate-keys` Befehl zum Festlegen des Zugriffsschlüssels und des Geheimschlüssels für diesen Benutzer.

> Verwenden Sie als NetApp Best Practice diesen Root-Benutzer nicht. Alle Client-Anwendungen, die den Zugriffsschlüssel oder den geheimen Schlüssel des Root-Benutzers verwenden, haben vollständigen Zugriff auf alle Buckets und Objekte im Objektspeicher.

Siehe `vserver object-store-server` Man-Pages für zusätzliche Konfigurations- und Anzeigeoptionen.

Beispiel 2. Schritte

System Manager

Gehen Sie folgendermaßen vor, wenn Sie einer vorhandenen Storage-VM einen S3-Server hinzufügen. Informationen zum Hinzufügen eines S3-Servers zu einer neuen Storage-VM finden Sie unter "Erstellung einer Storage-SVM für S3".

Sie sollten darauf vorbereitet sein, IP-Adressen für die Schnittstellenrollendaten einzugeben.

1. Aktivieren von S3 auf einer vorhandenen Storage-VM
   a. Wählen Sie die Speicher-VM aus: Klicken Sie auf **Storage > Storage VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann auf ⚙ Unter **S3**.
   b. Klicken Sie auf **S3** aktivieren und geben Sie dann den S3-Servernamen ein.
   c. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.

   d. Geben Sie die Netzwerkschnittstellen ein.
2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   - Der Geheimschlüssel wird nicht mehr angezeigt.
   - Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Erstellen des S3-Servers:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   Sie können weitere Optionen beim Erstellen des S3-Servers oder zu einem späteren Zeitpunkt festlegen.

   - Beim Konfigurieren von lokalem Tiering kann der SVM-Name entweder ein Daten-SVM- oder ein System-SVM-(Cluster-)Name sein.
   - Der Zertifikatname sollte der Name des Serverzertifikats (Endbenutzer- oder Leaf-Zertifikat) und nicht das Server-CA-Zertifikat (Zwischen- oder Stammzertifizierungsstellenzertifikat) sein.
   - HTTPS ist standardmäßig an Port 443 aktiviert. Sie können die Portnummer mit dem ändern `-secure-listener-port` Option.

     Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die korrekte Integration mit SSL/TLS erforderlich.

   - HTTP ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wartet der Server an Port 80. Aktivieren Sie die Aktivierung mit dem `-is-http-enabled` Oder ändern Sie die Portnummer mit `-listener-port` Option.

     Wenn HTTP aktiviert ist, werden die Anforderung und die Antworten im Klartext über das

Netzwerk gesendet.

2. Vergewissern Sie sich, dass S3 konfiguriert ist:

```
vserver object-store-server show
```

Beispiel

Mit diesem Befehl werden die Konfigurationswerte aller Objektspeicher-Server überprüft:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                     HTTP Enabled: false
                                    HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Fügen Sie einer S3-fähigen SVM Storage-Kapazität hinzu

Erstellen eines Buckets

S3 Objekte werden in *Buckets* aufbewahrt. Sie sind nicht als Dateien innerhalb eines Verzeichnisses in anderen Verzeichnissen verschachtelt.

Bevor Sie beginnen

Eine Storage-VM mit einem S3-Server muss bereits vorhanden sein.

Über diese Aufgabe

- Ab ONTAP 9.14.1 wurde die automatische Größenanpassung bei S3 FlexGroup Volumes beim Erstellen von Buckets aktiviert. So wird bei der Bucket-Erstellung auf vorhandenen und neuen FlexGroup Volumes keine übermäßige Kapazitätszuweisung mehr erreicht. Die Größe von FlexGroup Volumes wird anhand der folgenden Richtlinien auf die erforderliche Mindestgröße angepasst. Die erforderliche Mindestgröße ist die Gesamtgröße aller S3-Buckets in einem FlexGroup Volume.
  - Ab ONTAP 9.14.1 wird das FlexGroup Volume mit der minimal erforderlichen Größe erstellt, wenn ein S3-FlexGroup-Volume als Teil einer neuen Bucket-Erstellung erstellt wird.
  - Wenn ein S3-FlexGroup-Volume vor ONTAP 9.14.1 erstellt wurde, wird beim ersten, nach ONTAP 9.14.1 erstellten oder gelöschten Bucket das FlexGroup-Volume auf die minimal erforderliche Größe angepasst.
  - Wenn ein S3-FlexGroup-Volume vor ONTAP 9.14.1 erstellt wurde und bereits über die erforderliche Mindestgröße verfügt, bleibt beim Erstellen oder Löschen eines Buckets nach ONTAP 9.14.1 die Größe des S3-FlexGroup-Volumes erhalten.

- Storage-Service-Level sind vordefinierte Richtliniengruppen mit adaptiver Quality of Service (QoS) mit Standardeinstellungen wie *Value*, Performance_ und *extreme*. Anstelle eines der standardmäßigen Storage-Service-Level können Sie auch eine individuelle QoS-Richtliniengruppe definieren und auf einen Bucket anwenden. Weitere Informationen zu Speicherservicedefinitionen finden Sie unter "Definitionen von Storage-Services". Weitere Informationen zum Leistungsmanagement finden Sie unter "Performance Management". Ab ONTAP 9.8 ist bei der Bereitstellung von Storage QoS standardmäßig aktiviert. Sie können die QoS deaktivieren oder während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt eine individuelle QoS-Richtlinie auswählen.
- Wenn Sie lokales Kapazitäts-Tiering konfigurieren, erstellen Sie Buckets und Benutzer in einer Daten-Storage-VM und nicht in der System-Storage-VM, auf der sich der S3 Server befindet.
- Für den Remote-Client-Zugriff müssen Sie Buckets in einer S3-fähigen Storage-VM konfigurieren. Wenn Sie einen Bucket in einer Storage-VM erstellen, die nicht S3-aktiviert ist, ist dieser nur für lokales Tiering verfügbar.
- Ab ONTAP 9.14.1 ist dies möglich "Erstellung eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration".
- Wenn Sie für die CLI einen Bucket erstellen, haben Sie zwei Bereitstellungsoptionen:
  - Lassen Sie ONTAP Select die zugrunde liegenden Aggregate und FlexGroup Komponenten (Standard)
    - ONTAP erstellt und konfiguriert ein FlexGroup-Volume für den ersten Bucket durch die automatische Auswahl der Aggregate. Er wählt automatisch das höchste Service-Level aus, das für Ihre Plattform verfügbar ist, oder Sie können das Storage-Service-Level angeben. Alle zusätzlichen Buckets, die Sie später in der Storage-VM hinzufügen, verfügen über dasselbe zugrunde liegende FlexGroup Volume.
    - Alternativ können Sie angeben, ob der Bucket für das Tiering verwendet wird. In diesem Fall versucht ONTAP, kostengünstige Medien mit optimaler Performance für die Tiered-Daten auszuwählen.
  - Zudem wählen Sie die zugrunde liegenden Aggregate und FlexGroup-Komponenten aus (Optionen mit Advanced Privilege-Befehlen erforderlich): Sie können die Aggregate, auf denen der Bucket und das zugehörige FlexGroup Volume erstellt werden sollen, manuell auswählen und dann die Anzahl der Komponenten in jedem Aggregat angeben. Beim Hinzufügen weiterer Buckets:
    - Wenn Sie Aggregate und Komponenten für einen neuen Bucket angeben, wird für den neuen Bucket eine neue FlexGroup erstellt.
    - Wenn Sie keine Aggregate und Komponenten für einen neuen Bucket angeben, wird der neue Bucket zu einem vorhandenen FlexGroup hinzugefügt. Siehe Management von FlexGroup Volumes Finden Sie weitere Informationen.

      Wenn bei der Erstellung eines Buckets Aggregate und Komponenten angegeben werden, werden keine QoS-Richtliniengruppen oder Benutzerdefiniert angewendet. Dies können Sie später mit dem tun `vserver object-store-server bucket modify` Befehl.

  Siehe "vserver Objekt-Store-Server Bucket ändern" Finden Sie weitere Informationen.

Hinweis: Wenn Sie Eimer von Cloud Volumes ONTAP bedienen, sollten Sie das CLI-Verfahren verwenden. Es wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Node verwenden. Die Verwendung von Aggregaten beider Nodes kann sich auf die Performance auswirken, da die Nodes sich in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind.

Erstellen von S3 Buckets mit der ONTAP-CLI

1. Wenn Sie Aggregate und FlexGroup Komponenten selbst auswählen möchten, setzen Sie die Berechtigungsebene auf „Advanced“ (ansonsten reicht die Admin-Berechtigungsebene aus): `set -privilege advanced`
2. Erstellen eines Buckets:

   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

   Der Name der Storage VM kann entweder eine Daten-Storage-VM oder sein `Cluster` (Der Name der System-Storage-VM), wenn Sie lokales Tiering konfigurieren.

   Wenn Sie keine Optionen angeben, erstellt ONTAP einen Bucket mit 800 GB mit dem Service Level auf das höchste für das System verfügbare Level.

   Wenn ONTAP einen Bucket auf Basis der Performance oder Auslastung erstellen soll, verwenden Sie eine der folgenden Optionen:

   - Service-Level

     Nehmen Sie die auf `-storage-service-level` Option mit einem der folgenden Werte: `value`, `performance`, Oder `extreme`.

   - tiering

     Nehmen Sie die auf `-used-as-capacity-tier true` Option.

     Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, verwenden Sie die folgenden Optionen:

   - Der `-aggr-list` Der Parameter gibt die Liste der Aggregate an, die für FlexGroup Volume-Komponenten verwendet werden sollen.

     Jeder Eintrag in der Liste erstellt eine Komponente im angegebenen Aggregat. Sie können ein Aggregat mehrmals angeben, damit mehrere Komponenten auf dem Aggregat erstellt werden.

   Für eine konsistente Performance im FlexGroup Volume müssen alle Aggregate denselben Festplattentyp und dieselbe Konfiguration der RAID-Gruppen verwenden.

   - Der `-aggr-list-multiplier` Parameter gibt die Anzahl der Wiederholungen über die Aggregate an, die mit dem aufgeführt sind `-aggr-list` Parameter beim Erstellen eines FlexGroup-Volumes.

     Der Standardwert des `-aggr-list-multiplier` Der Parameter ist 4.

3. Fügen Sie bei Bedarf eine QoS-Richtliniengruppe hinzu:

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Überprüfen der Bucket-Erstellung:

   `vserver object-store-server bucket show [-instance]`

Beispiel

Im folgenden Beispiel wird ein Bucket für Storage-VM erstellt `vs1` Der Größe `1TB` Und Angabe des Aggregats:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Erstellung von S3 Buckets mit System Manager

1. Fügen Sie auf einer S3-fähigen Storage-VM einen neuen Bucket hinzu.
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.
      - Wenn Sie an dieser Stelle auf **Speichern** klicken, wird ein Bucket mit den folgenden Standardeinstellungen erstellt:
        - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, bereits Gruppenrichtlinien sind gültig.

          Sie sollten den S3-Root-Benutzer nicht zum Managen von ONTAP-Objekt-Storage und zur gemeinsamen Nutzung seiner Berechtigungen verwenden, da er unbegrenzten Zugriff auf den Objektspeicher hat. Erstellen Sie stattdessen einen Benutzer oder eine Gruppe mit Administratorrechten, die Sie zuweisen.

        - Das Niveau der Servicequalität (Performance) ist das höchste für Ihr System verfügbare Niveau.
      - Klicken Sie auf **Speichern**, um einen Bucket mit diesen Standardwerten zu erstellen.

Konfigurieren Sie zusätzliche Berechtigungen und Einschränkungen

Sie können auf **Weitere Optionen** klicken, um Einstellungen für Objektsperrung, Benutzerberechtigungen und Leistungslevel zu konfigurieren, wenn Sie den Bucket konfigurieren, oder Sie können diese Einstellungen später ändern.

Wenn Sie beabsichtigen, den S3-Objektspeicher für FabricPool Tiering zu nutzen, sollten Sie die Wahl erwägen **für Tiering** zu verwenden (kostengünstige Medien mit optimaler Performance für die Tiered Data verwenden) anstatt ein Performance-Service-Level.

Wenn Sie die Versionierung für Ihre Objekte für eine spätere Wiederherstellung aktivieren möchten, wählen Sie **Versionierung aktivieren**. Die Versionierung ist standardmäßig aktiviert, wenn Sie die Objektsperrung auf dem Bucket aktivieren. Informationen zur Objektversionierung finden Sie im "Verwenden von Versionierung in S3 Buckets für Amazon".

Ab Version 9.14.1 wird die Objektsperrung in S3 Buckets unterstützt. Für die S3 Objektsperrung ist eine standardmäßige SnapLock-Lizenz erforderlich. Diese Lizenz ist in enthalten "ONTAP One". Vor ONTAP One war die SnapLock-Lizenz im Paket für Sicherheit und Compliance enthalten. Das Paket „Sicherheit und Compliance“ wird nicht mehr angeboten, ist aber weiterhin gültig. Bestehende Kunden können diese Option wählen, obwohl sie derzeit nicht benötigt werden "Upgrade auf ONTAP One". Wenn Sie die Objektsperrung für einen Bucket aktivieren, sollten Sie dies tun "Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist". Wenn keine SnapLock-Lizenz installiert ist, müssen Sie dies tun "Installieren" Bevor Sie die Objektsperrung aktivieren können. Wenn Sie die Installation der SnapLock-Lizenz überprüft haben, wählen Sie **enable object locking** aus, um Objekte in Ihrem Bucket vor dem Löschen oder Überschreiben zu schützen. Die Sperrung

kann entweder für alle oder für bestimmte Objektversionen aktiviert werden und nur dann, wenn die SnapLock-Compliance-Uhr für die Cluster-Nodes initialisiert wird. Führen Sie hierzu folgende Schritte aus:

1. Wenn die SnapLock-Compliance-Uhr auf keinem Knoten des Clusters initialisiert wird, wird die Schaltfläche **SnapLock-Compliance-Uhr initialisieren** angezeigt. Klicken Sie auf **SnapLock-Compliance-Uhr initialisieren**, um die SnapLock-Compliance-Uhr auf den Clusterknoten zu initialisieren.
2. Wählen Sie den Modus **Governance**, um eine zeitbasierte Sperre zu aktivieren, die *Write Once, Read Many (WORM)* Berechtigungen für die Objekte erlaubt. Selbst im *Governance*-Modus können die Objekte von Administratorbenutzern mit bestimmten Berechtigungen gelöscht werden.
3. Wählen Sie **Compliance**-Modus, wenn Sie strengere Regeln für die Löschung und Aktualisierung der Objekte zuweisen möchten. In diesem Modus der Objektsperrung können die Objekte nur nach Abschluss der angegebenen Aufbewahrungsfrist abgelaufen sein. Sofern keine Aufbewahrungsfrist festgelegt ist, bleiben die Objekte unbegrenzt gesperrt.
4. Geben Sie die Aufbewahrungsfrist für die Sperre in Tagen oder Jahren an, wenn die Verriegelung für einen bestimmten Zeitraum wirksam sein soll.

> Das Sperren gilt für S3-Buckets mit Versionsangabe und ohne Versionsangabe. Objektsperrung gilt nicht für NAS-Objekte.

Sie können Sicherungs- und Berechtigungseinstellungen sowie Performance Service Level für den Bucket konfigurieren.

> Sie müssen bereits Benutzer und Gruppen erstellt haben, bevor Sie die Berechtigungen konfigurieren.

Weitere Informationen finden Sie unter "Spiegelung für neuen Bucket erstellen".

Überprüfen Sie den Zugriff auf den Bucket

Für S3-Client-Applikationen (ob ONTAP S3 oder eine externe Drittanbieterapplikation) können Sie Ihren Zugriff auf den neu erstellten Bucket überprüfen, indem Sie Folgendes eingeben:

- Das S3-Server-CA-Zertifikat.
- Der Zugriffsschlüssel und der geheime Schlüssel des Benutzers.
- Der FQDN-Name des S3-Servers und der Bucket-Name.

Erstellung eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration

Ab ONTAP 9.14.1 können Sie einen Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in MetroCluster FC- und IP-Konfigurationen bereitstellen.

Über diese Aufgabe

- Standardmäßig werden Buckets für gespiegelte Aggregate bereitgestellt.
- Dieselben Bereitstellungsrichtlinien wie in beschrieben "Erstellen eines Buckets" Anwenden bei der Erstellung eines Buckets in einer MetroCluster-Umgebung.
- Die folgenden S3-Objekt-Storage-Funktionen werden in MetroCluster Umgebungen **nicht** unterstützt:
  - S3 SnapMirror

- S3 Bucket-Lifecycle-Management
- S3-Objektsperre im **Compliance**-Modus

  S3-Objektsperre im **Governance**-Modus wird unterstützt.

- Lokales FabricPool Tiering

Bevor Sie beginnen

Eine SVM, die einen S3-Server enthält, muss bereits vorhanden sein.

Erstellung von Buckets wird verarbeitet

CLI

1. Wenn Sie Aggregate und FlexGroup Komponenten selbst auswählen möchten, setzen Sie die Berechtigungsebene auf „Advanced“ (ansonsten reicht die Admin-Berechtigungsebene aus): `set -privilege advanced`
2. Erstellen eines Buckets:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   Stellen Sie die ein `-use-mirrored-aggregates` Option auf `true` Oder `false` Je nachdem, ob Sie ein gespiegeltes oder nicht gespiegeltes Aggregat verwenden möchten.

   > Standardmäßig wird der verwendet `-use-mirrored-aggregates` Die Option ist auf festgelegt `true`.

   - Der SVM-Name muss eine Daten-SVM sein.
   - Wenn Sie keine Optionen angeben, erstellt ONTAP einen Bucket mit 800 GB mit dem Service Level auf das höchste für das System verfügbare Level.
   - Wenn ONTAP einen Bucket auf Basis der Performance oder Auslastung erstellen soll, verwenden Sie eine der folgenden Optionen:
     - Service-Level

       Nehmen Sie die auf `-storage-service-level` Option mit einem der folgenden Werte: `value`, `performance`, Oder `extreme`.

     - tiering

       Nehmen Sie die auf `-used-as-capacity-tier true` Option.
   - Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, verwenden Sie die folgenden Optionen:
     - Der `-aggr-list` Der Parameter gibt die Liste der Aggregate an, die für FlexGroup Volume-Komponenten verwendet werden sollen.

       Jeder Eintrag in der Liste erstellt eine Komponente im angegebenen Aggregat. Sie können ein Aggregat mehrmals angeben, damit mehrere Komponenten auf dem Aggregat erstellt werden.

   Für eine konsistente Performance im FlexGroup Volume müssen alle Aggregate denselben Festplattentyp und dieselbe Konfiguration der RAID-Gruppen verwenden.

   - Der `-aggr-list-multiplier` Parameter gibt die Anzahl der Wiederholungen über die Aggregate an, die mit dem aufgeführt sind `-aggr-list` Parameter beim Erstellen eines FlexGroup-Volumes.

     Der Standardwert des `-aggr-list-multiplier` Der Parameter ist 4.

3. Fügen Sie bei Bedarf eine QoS-Richtliniengruppe hinzu:

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   ```

```
-group qos_policy_group
```

4. Überprüfen der Bucket-Erstellung:

```
vserver object-store-server bucket show [-instance]
```

Beispiel

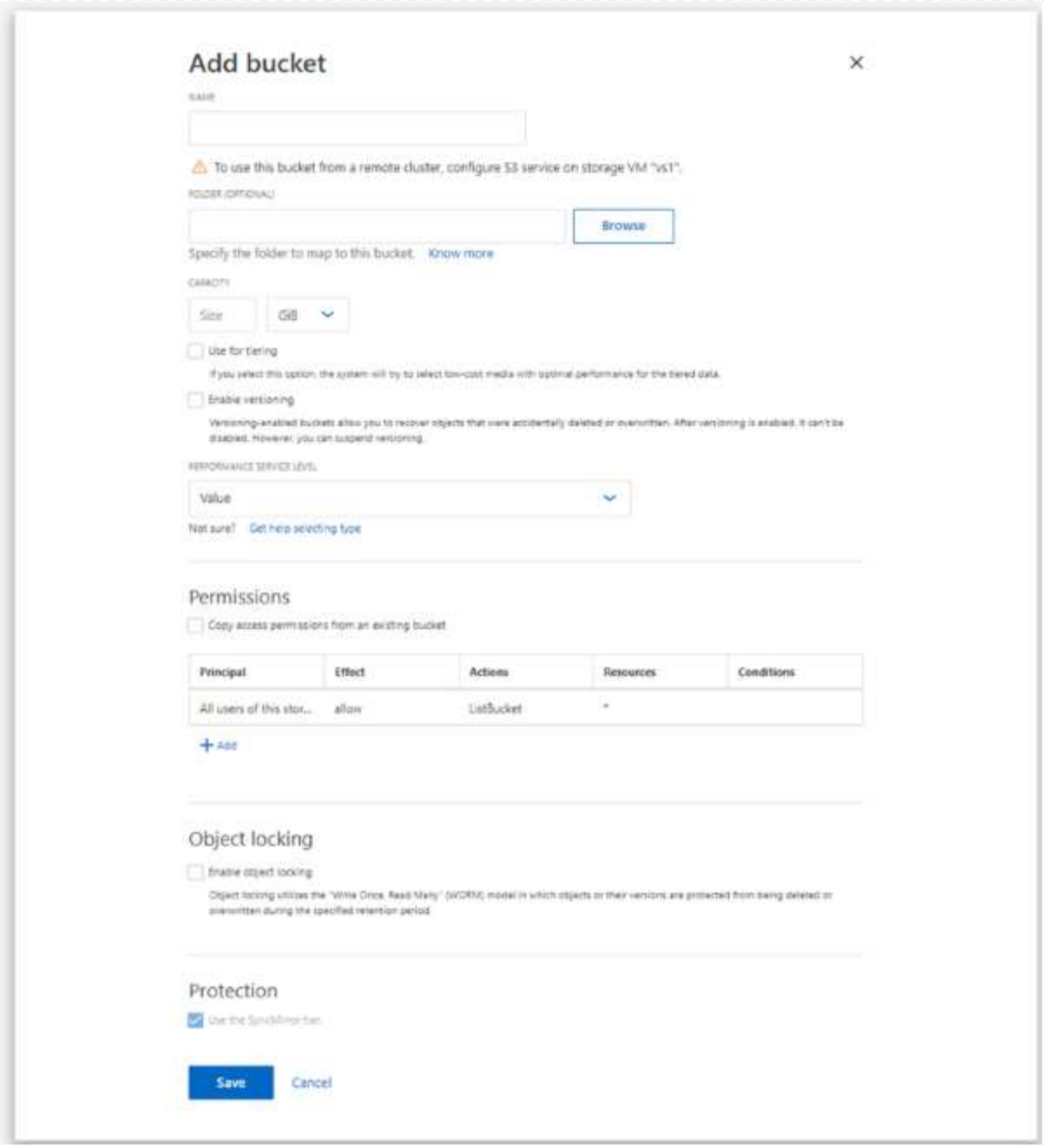
Im folgenden Beispiel wird ein Bucket für SVM vs1 mit der Größe 1 TB auf einem gespiegelten Aggregat erstellt:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Fügen Sie auf einer S3-fähigen Storage-VM einen neuen Bucket hinzu.
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

      Standardmäßig wird der Bucket auf einem gespiegelten Aggregat bereitgestellt. Wenn Sie einen Bucket auf einem nicht gespiegelten Aggregat erstellen möchten, wählen Sie **Weitere Optionen** und deaktivieren Sie das Kontrollkästchen **Use the SyncMirror Tier** unter **Schutz** wie im folgenden Bild gezeigt:



- Wenn Sie an dieser Stelle auf **Speichern** klicken, wird ein Bucket mit den folgenden Standardeinstellungen erstellt:
  - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, bereits Gruppenrichtlinien sind gültig.

    Sie sollten den S3-Root-Benutzer nicht zum Managen von ONTAP-Objekt-Storage und zur gemeinsamen Nutzung seiner Berechtigungen verwenden, da er unbegrenzten Zugriff auf den Objektspeicher hat. Erstellen Sie stattdessen einen Benutzer oder eine Gruppe mit Administratorrechten, die Sie zuweisen.

  - Das Niveau der Servicequalität (Performance) ist das höchste für Ihr System verfügbare Niveau.

- Sie können auf **Weitere Optionen** klicken, um Benutzerberechtigungen und Leistungslevel zu konfigurieren, wenn Sie den Bucket konfigurieren, oder Sie können diese Einstellungen später ändern.
  - Sie müssen bereits Benutzer und Gruppen erstellt haben, bevor Sie **Weitere Optionen** verwenden, um ihre Berechtigungen zu konfigurieren.
  - Wenn Sie beabsichtigen, den S3-Objektspeicher für FabricPool Tiering zu nutzen, sollten Sie die Wahl erwägen **für Tiering** zu verwenden (kostengünstige Medien mit optimaler Performance für die Tiered Data verwenden) anstatt ein Performance-Service-Level.

2. Überprüfen Sie bei S3-Client-Applikationen – einem anderen ONTAP System oder einer externen App von Drittanbietern – den Zugriff auf den neuen Bucket, indem Sie Folgendes eingeben:
   - Das S3-Server-CA-Zertifikat.
   - Der Zugriffsschlüssel und der Geheimschlüssel des Benutzers.
   - Der FQDN-Name des S3-Servers und der Bucket-Name.

Erstellen einer Bucket-Lifecycle-Management-Regel

Ab ONTAP 9.13.1 können Sie Lifecycle-Managementregeln erstellen, um Objekt-Lebenszyklen in Ihren S3 Buckets zu managen. Sie können Löschregeln für bestimmte Objekte in einem Bucket definieren und diese Bucket-Objekte durch diese Regeln ablaufen lassen. So können Sie Datenhaltungsanforderungen erfüllen und den gesamten S3 Objekt-Storage effizient managen.

> Wenn die Objektsperrung für Ihre Bucket-Objekte aktiviert ist, werden die Lifecycle-Management-Regeln für die Objektablauffrist nicht auf gesperrte Objekte angewendet. Informationen zur Objektsperrung finden Sie unter "Erstellen eines Buckets".

Bevor Sie beginnen

Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits vorhanden sein. Siehe "Erstellung einer SVM für S3" Finden Sie weitere Informationen.

Über diese Aufgabe

Beim Erstellen von Lifecycle-Management-Regeln können Sie die folgenden Löschaktionen auf Ihre Bucket-Objekte anwenden:

- Löschen aktueller Versionen – Diese Aktion läuft Objekte ab, die durch die Regel identifiziert werden. Wenn die Versionierung auf dem Bucket aktiviert ist, sind alle abgelaufenen Objekte in S3 nicht verfügbar. Wenn die Versionierung nicht aktiviert ist, werden die Objekte durch diese Regel dauerhaft gelöscht. Die CLI-Aktion ist `Expiration`.
- Löschen nicht aktueller Versionen – Diese Aktion gibt an, wann S3 nicht aktuelle Objekte dauerhaft entfernen kann. Die CLI-Aktion ist `NoncurrentVersionExpiration`.
- Löschen abgelaufener Löschmarkierungen - Diese Aktion löscht abgelaufene Löschmarkierungen von Objekten. In versionierungsfähigen Buckets werden Objekte mit Löschmarkierungen zu den aktuellen Versionen der Objekte. Die Objekte werden nicht gelöscht, und es kann keine Aktion für sie ausgeführt werden. Diese Objekte sind abgelaufen, wenn ihnen keine aktuellen Versionen zugeordnet sind. Die CLI-Aktion ist `Expiration`.
- Löschen von unvollständigen mehrteiligen Uploads: Mit dieser Aktion wird die maximale Zeit (in Tagen) festgelegt, die Sie zulassen möchten, dass mehrteilige Uploads noch ausgeführt werden. Danach werden

sie gelöscht. Die CLI-Aktion ist `AbortIncompleteMultipartUpload`.

Die Vorgehensweise, die Sie befolgen, hängt von der verwendeten Schnittstelle ab. Bei ONTAP 9.13,1 müssen Sie die CLI verwenden. Ab ONTAP 9.14.1 können Sie auch System Manager verwenden.

Verwalten Sie Lifecycle Management-Regeln mit der CLI

Ab ONTAP 9.13.1 können Sie über die ONTAP CLI Lifecycle-Managementregeln erstellen, um Objekte in Ihren S3 Buckets ablaufen zu lassen.

Bevor Sie beginnen

Für die CLI müssen Sie die erforderlichen Felder für jeden Ablaufaktionstyp definieren, wenn Sie eine Bucket-Lebenszyklusverwaltungsregel erstellen. Diese Felder können nach der ersten Erstellung geändert werden. In der folgenden Tabelle werden die eindeutigen Felder für jeden Aktionstyp angezeigt.

Aktionstyp	Eindeutige Felder
NichtCurrentVersionAblauf	• `-non-curr-days` - Anzahl der Tage, nach denen nicht aktuelle Versionen gelöscht werden • `-new-non-curr-versions` - Anzahl der neuesten nicht-aktuellen Versionen, die beibehalten werden sollen
Ablauf	• `-obj-age-days` - Anzahl der Tage seit der Erstellung, nach denen die aktuelle Version der Objekte gelöscht werden kann • `-obj-exp-date` - Bestimmtes Datum, wann die Objekte ablaufen sollen • `-expired-obj-del-markers` - Löschen von Objektmarkierungen
AbortInsetteMultipartUpload	• `-after-initiation-days` - Anzahl der Tage der Initiierung, nach denen der Upload abgebrochen werden kann

Damit die Bucket-Lifecycle-Management-Regel nur auf eine bestimmte Untergruppe von Objekten angewendet werden kann, müssen Administratoren beim Erstellen der Regel jeden Filter festlegen. Wenn diese Filter beim Erstellen der Regel nicht festgelegt werden, wird die Regel auf alle Objekte innerhalb des Buckets angewendet.

Alle Filter können nach der ersten Erstellung geändert werden *außer* für Folgendes:

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Schritte

1. Verwenden Sie die `vserver object-store-server bucket lifecycle-management-rule create` Befehl mit den erforderlichen Feldern für Ihren Ablaufaktionstyp, um Ihre Bucket-Lifecycle-Management-Regel zu erstellen.

Beispiel

Mit dem folgenden Befehl wird eine Lebenszyklusverwaltungsregel für den Bucket „NonCurrentVersionExpiration“ erstellt:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Beispiel

Mit dem folgenden Befehl wird eine Management-Regel für AblaufBucket-Lebenszyklus erstellt:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Beispiel

Mit dem folgenden Befehl wird eine AbortIncompleMultipartUpload Bucket Lifecycle Management-Regel erstellt:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Managen Sie Lifecycle Management-Regeln mit System Manager

Ab ONTAP 9.14.1 können Sie S3 Objekte mit System Manager ablaufen lassen. Sie können Lifecycle-Management-Regeln für Ihre S3-Objekte hinzufügen, bearbeiten und löschen. Darüber hinaus können Sie eine für einen Bucket erstellte Lebenszyklusregel importieren und für die Objekte in einem anderen Bucket nutzen. Sie können eine aktive Regel deaktivieren und später aktivieren.

Fügen Sie eine Lebenszyklusverwaltungsregel hinzu

1. Klicken Sie Auf **Speicher > Buckets**.
2. Wählen Sie den Bucket aus, für den Sie die Ablaufregel festlegen möchten.

3. Klicken Sie auf das ⋮ Und wählen Sie **Lebenszyklusregeln verwalten**.
4. Klicken Sie auf **Hinzufügen > Lebenszyklusregel**.
5. Fügen Sie auf der Seite Lebenszyklusregel hinzufügen den Namen der Regel hinzu.
6. Definieren Sie den Geltungsbereich der Regel, unabhängig davon, ob sie auf alle Objekte im Bucket oder auf bestimmte Objekte angewendet werden soll. Wenn Sie Objekte angeben möchten, fügen Sie mindestens eines der folgenden Filterkriterien hinzu:
   a. Präfix: Geben Sie ein Präfix der Objektschlüsselnamen an, auf die die Regel angewendet werden soll. Normalerweise handelt es sich um den Pfad oder Ordner des Objekts. Sie können pro Regel ein Präfix eingeben. Sofern kein gültiges Präfix angegeben wird, gilt die Regel für alle Objekte in einem Bucket.
   b. Tags: Geben Sie bis zu drei Schlüssel- und Wertpaare (Tags) für die Objekte an, auf die die Regel angewendet werden soll. Zum Filtern werden nur gültige Schlüssel verwendet. Der Wert ist optional. Wenn Sie jedoch Werte hinzufügen, stellen Sie sicher, dass Sie nur gültige Werte für die entsprechenden Schlüssel hinzufügen.
   c. Größe: Sie können den Umfang zwischen der minimalen und maximalen Größe der Objekte begrenzen. Sie können einen oder beide Werte eingeben. Die Standardeinheit ist MiB.
7. Geben Sie die Aktion an:
   a. **Die aktuelle Version von Objekten ablaufen lassen**: Legen Sie eine Regel fest, um alle aktuellen Objekte nach einer bestimmten Anzahl von Tagen seit ihrer Erstellung oder an einem bestimmten Datum dauerhaft nicht mehr verfügbar zu machen. Diese Option ist nicht verfügbar, wenn die Option **Delete Expired object delete Markers** ausgewählt ist.
   b. **Nicht aktuelle Versionen dauerhaft löschen**: Geben Sie die Anzahl der Tage an, nach denen die Version nicht aktuell wird, und danach kann gelöscht werden, und die Anzahl der zu haltenden Versionen.
   c. **Löschen abgelaufener Objektlösch-Marker**: Wählen Sie diese Aktion, um Objekte mit abgelaufenen Löschmarkierungen zu löschen, d.h. Marker ohne zugeordnetes aktuelles Objekt zu löschen.

      ⓘ Diese Option ist nicht mehr verfügbar, wenn Sie die Option **die aktuelle Version von Objekten ablaufen lassen** auswählen, die automatisch alle Objekte nach der Aufbewahrungsfrist löscht. Diese Option ist auch nicht mehr verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.

   d. **Unvollständige mehrteilige Uploads löschen**: Legen Sie die Anzahl der Tage fest, nach denen unvollständige mehrteilige Uploads gelöscht werden sollen. Wenn die mehrteiligen Uploads, die gerade ausgeführt werden, innerhalb der angegebenen Aufbewahrungsfrist fehlschlagen, können Sie die unvollständigen mehrteiligen Uploads löschen. Diese Option ist nicht mehr verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.
   e. Klicken Sie Auf **Speichern**.

Lebenszyklusregel importieren

1. Klicken Sie Auf **Speicher > Buckets**.
2. Wählen Sie den Bucket aus, für den Sie die Ablaufregel importieren möchten.
3. Klicken Sie auf das ⋮ Und wählen Sie **Lebenszyklusregeln verwalten**.
4. Klicken Sie auf **Hinzufügen > Regel importieren**.
5. Wählen Sie den Bucket aus, aus dem Sie die Regel importieren möchten. Die für den ausgewählten Bucket definierten Lifecycle-Management-Regeln werden angezeigt.

6. Wählen Sie die Regel aus, die Sie importieren möchten. Sie haben die Möglichkeit, jeweils eine Regel auszuwählen, wobei die Standardauswahl die erste Regel ist.
7. Klicken Sie Auf **Import**.

Bearbeiten, löschen oder deaktivieren Sie eine Regel

Sie können nur die Lifecycle-Management-Aktionen bearbeiten, die der Regel zugeordnet sind. Wenn die Regel mit Objekt-Tags gefiltert wurde, stehen die Optionen **abgelaufene Objekte löschen Marker** und **unvollständige mehrteilige Uploads löschen** nicht zur Verfügung.

Wenn Sie eine Regel löschen, gilt diese Regel nicht mehr für zuvor zugeordnete Objekte.

1. Klicken Sie Auf **Speicher > Buckets**.
2. Wählen Sie den Bucket aus, für den Sie die Lifecycle-Management-Regel bearbeiten, löschen oder deaktivieren möchten.
3. Klicken Sie auf das ⋮ Und wählen Sie **Lebenszyklusregeln verwalten**.
4. Wählen Sie die gewünschte Regel aus. Sie können jeweils eine Regel bearbeiten und deaktivieren. Sie können mehrere Regeln auf einmal löschen.
5. Wählen Sie **Bearbeiten**, **Löschen** oder **Deaktivieren**, und schließen Sie das Verfahren ab.

Erstellen eines S3-Benutzers

Für alle ONTAP-Objektspeicher ist eine Benutzerautorisierung erforderlich, um die Konnektivität zu autorisierten Clients einzuschränken.

Bevor Sie beginnen.

Eine S3-fähige Storage-VM muss bereits vorhanden sein.

Über diese Aufgabe

Ein S3-Benutzer kann Zugriff auf jeden Bucket in einer Storage-VM erhalten. Wenn Sie einen S3-Benutzer erstellen, werden auch ein Zugriffsschlüssel und ein geheimer Schlüssel für den Benutzer generiert. Sie sollten zusammen mit dem FQDN des Objektspeichers und dem Bucket-Namen für den Benutzer freigegeben werden. Die Schlüssel eines S3-Benutzers können mit dem angezeigt werden `vserver object-store-server user show` Befehl.

Sie können S3 Benutzern in einer Bucket-Richtlinie oder einer Objekt-Server-Richtlinie spezifische Zugriffsberechtigungen zuweisen.

> ⓘ Wenn Sie einen neuen Objektspeicher-Server erstellen, erstellt ONTAP einen Root-Benutzer (UID 0), ein privilegierter Benutzer mit Zugriff auf alle Buckets. Anstatt ONTAP S3 als Root-Benutzer zu verwalten, empfiehlt NetApp, eine Admin-Benutzerrolle mit bestimmten Berechtigungen zu erstellen.

CLI

1. S3-Benutzer erstellen:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - Das Hinzufügen eines Kommentars ist optional.
   - Ab ONTAP 9.14.1 können Sie den Zeitraum festlegen, für den der Schlüssel in gültig sein wird `-key-time-to-live` Parameter. Sie können den Aufbewahrungszeitraum in diesem Format hinzufügen, um den Zeitraum anzugeben, nach dem der Zugriffsschlüssel abläuft: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Wenn Sie beispielsweise eine Aufbewahrungsfrist von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingeben möchten, geben Sie den Wert als ein `P1DT2H3M4S`. Sofern nicht angegeben, ist der Schlüssel für einen unbestimmten Zeitraum gültig.

     Im folgenden Beispiel wird ein Benutzer mit dem Namen erstellt `sm_user1` Auf Storage-VM `vs0`, Mit einer Schlüsselaufbewahrungsfrist von einer Woche.

   ```
   vserver object-store-server user create -vserver vs0 -user sm_user1
   -key-time-to-live P1W
   ```

2. Achten Sie darauf, den Zugriffsschlüssel und den geheimen Schlüssel zu speichern. Sie werden für den Zugriff von S3-Clients benötigt.

System Manager

1. Klicken Sie auf **Storage > Storage VMs**. Wählen Sie die Speicher-VM aus, zu der Sie einen Benutzer hinzufügen möchten, wählen Sie **Einstellungen** und klicken Sie dann auf Unter S3.
2. Um einen Benutzer hinzuzufügen, klicken Sie auf **Benutzer > Hinzufügen**.
3. Geben Sie einen Namen für den Benutzer ein.
4. Ab ONTAP 9.14.1 können Sie den Aufbewahrungszeitraum der Zugriffsschlüssel festlegen, die für den Benutzer erstellt werden. Sie können den Aufbewahrungszeitraum in Tagen, Stunden, Minuten oder Sekunden angeben, nach denen die Schlüssel automatisch ablaufen. Standardmäßig ist der Wert auf festgelegt `0` Das bedeutet, dass der Schlüssel unbegrenzt gültig ist.
5. Klicken Sie Auf **Speichern**. Der Benutzer wird erstellt, und ein Zugriffsschlüssel und ein geheimer Schlüssel werden für den Benutzer generiert.
6. Laden Sie den Zugriffsschlüssel und den geheimen Schlüssel herunter, oder speichern Sie ihn. Sie werden für den Zugriff von S3-Clients benötigt.

Nächste Schritte

- Erstellen oder Ändern von S3-Gruppen

Erstellen oder Ändern von S3-Gruppen

Sie können den Bucket-Zugriff vereinfachen, indem Sie Benutzergruppen mit entsprechenden Zugriffsberechtigungen erstellen.

Bevor Sie beginnen

S3-Benutzer in einer S3-fähigen SVM müssen bereits vorhanden sein.

Über diese Aufgabe

Benutzern in einer S3-Gruppe kann Zugriff auf jeden Bucket in einer SVM, nicht aber auf mehrere SVMs gewährt werden. Gruppenzugriffsberechtigungen können auf zwei Arten konfiguriert werden:

- Auf Bucket-Ebene

  Nachdem Sie eine Gruppe von S3-Benutzern erstellt haben, geben Sie in den Bucket-Richtlinienerklärungen Gruppenberechtigungen an, die nur auf diesen Bucket angewendet werden.

- Auf SVM-Ebene

  Nach dem Erstellen einer Gruppe von S3-Benutzern geben Sie in der Gruppendefinition die Namen der Objektserverrichtlinien an. Diese Richtlinien bestimmen die Buckets und den Zugriff für die Gruppenmitglieder.

System Manager

1. Bearbeiten Sie den Speicher-VM: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf Unter S3.
2. Fügen Sie eine Gruppe hinzu: Wählen Sie **Gruppen** und dann **Hinzufügen**.
3. Geben Sie einen Gruppennamen ein, und wählen Sie aus einer Benutzerliste aus.
4. Sie können eine vorhandene Gruppenrichtlinie auswählen oder eine jetzt hinzufügen oder später eine Richtlinie hinzufügen.

CLI

1. Erstellen einer S3-Gruppe:
   `vserver object-store-server group create -vserver` *`svm_name`* `-name` *`group_name`* `-users` *`user_name\(s\)`* `[-policies` *`policy_names`*`] [-comment` *`text`*`\]`Der `-policies` Option kann in Konfigurationen mit nur einem Bucket in einem Objektspeicher weggelassen werden; der Gruppenname kann der Bucket-Richtlinie hinzugefügt werden. Der `-policies` Option kann später mit der hinzugefügt werden `vserver object-store-server group modify` Befehl nach Erstellung der Objekt-Storage-Server-Richtlinien

Schlüssel neu generieren und Aufbewahrungsfrist ändern

Zugriffsschlüssel und geheime Schlüssel werden automatisch während der Erstellung von Benutzern generiert, um den S3-Client-Zugriff zu ermöglichen. Sie können Schlüssel für einen Benutzer neu generieren, wenn ein Schlüssel abgelaufen ist oder kompromittiert wurde.

Informationen zur Generierung von Zugriffsschlüsseln finden Sie unter "Erstellen eines S3-Benutzers".

CLI

1. Regenerieren Sie Zugriff und geheime Schlüssel für einen Benutzer, indem Sie den ausführen `vserver object-store-server user regenerate-keys` Befehl.
2. Generierte Schlüssel sind standardmäßig für unbegrenzte Zeit gültig. Ab 9.14.1 können Sie die Aufbewahrungsfrist ändern, nach der die Schlüssel automatisch ablaufen. Sie können den Aufbewahrungszeitraum in diesem Format hinzufügen: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Wenn Sie beispielsweise eine Aufbewahrungsfrist von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingeben möchten, geben Sie den Wert als ein `P1DT2H3M4S`.

```
vserver object-store-server user regenerate-keys -vserver svm_name
-user user -key-time-to-live 0
```

3. Speichern Sie den Zugriff und die geheimen Schlüssel. Sie werden für den Zugriff von S3-Clients benötigt.

System Manager

1. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf In der Kachel **S3**.
3. Überprüfen Sie auf der Registerkarte **Users**, ob kein Zugriffsschlüssel vorhanden ist oder der Schlüssel für den Benutzer abgelaufen ist.
4. Wenn Sie den Schlüssel neu generieren möchten, klicken Sie auf Klicken Sie neben dem Benutzer auf **Schlüssel neu generieren**.
5. Generierte Schlüssel sind standardmäßig für eine unbestimmte Zeit gültig. Ab 9.14.1 können Sie die Aufbewahrungsfrist ändern, nach der die Schlüssel automatisch ablaufen. Geben Sie den Aufbewahrungszeitraum in Tagen, Stunden, Minuten oder Sekunden ein.
6. Klicken Sie Auf **Speichern**. Der Schlüssel wird neu generiert. Jede Änderung der Schlüsselaufbewahrungsfrist tritt unmittelbar in Kraft.
7. Laden Sie den Zugriffsschlüssel und den geheimen Schlüssel herunter, oder speichern Sie ihn. Sie werden für den Zugriff von S3-Clients benötigt.

Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen

Allgemeines zu Bucket- und Objektspeicherserverrichtlinien

Benutzer- und Gruppenzugriff auf S3-Ressourcen wird über Bucket- und Objektspeicher-Serverrichtlinien gesteuert. Wenn Sie eine kleine Anzahl von Benutzern oder Gruppen haben, ist die Kontrolle des Zugriffs auf Bucket-Ebene wahrscheinlich ausreichend, aber wenn Sie viele Benutzer und Gruppen haben, ist es einfacher, den Zugriff auf der Objektspeicherserverebene zu steuern.

Ändern einer Bucket-Richtlinie

Zugriffsregeln können zur Standard-Bucket-Richtlinie hinzugefügt werden. Der Umfang

seiner Zugriffssteuerung umfasst den Bucket, der im EinzelBucket enthalten ist, daher ist er am besten geeignet.

Bevor Sie beginnen

Eine S3-fähige Storage-VM muss bereits vorhanden sein, die einen S3-Server und einen Bucket enthält.

Sie müssen bereits Benutzer oder Gruppen erstellt haben, bevor Sie Berechtigungen erteilen.

Über diese Aufgabe

Sie können neue Anweisungen für neue Benutzer und Gruppen hinzufügen oder die Attribute vorhandener Anweisungen ändern. Weitere Optionen finden Sie im `vserver object-store-server bucket policy` Man-Pages.

Benutzer- und Gruppenberechtigungen können bei Erstellung des Buckets oder nach Bedarf später zugewiesen werden. Sie können auch die Bucket-Kapazität und die QoS-Richtliniengruppenzuweisung ändern.

Ab ONTAP 9.9 unterstützen Sie die Objekt-Tagging-Funktionen von AWS für Clients mit dem ONTAP S3-Server `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging` Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Schritte

1. Bearbeiten Sie den Bucket: Klicken Sie auf **Storage > Buckets**, klicken Sie auf den gewünschten Bucket und klicken Sie dann auf **Bearbeiten**. Beim Hinzufügen oder Ändern von Berechtigungen können Sie die folgenden Parameter angeben:
   - **Auftraggeber**: Der Benutzer oder die Gruppe, auf die der Zugriff gewährt wird.
   - **Effekt**: Erlaubt oder verweigert den Zugriff auf einen Benutzer oder eine Gruppe.
   - **Aktionen**: Zulässige Aktionen im Bucket für einen bestimmten Benutzer oder eine bestimmte Gruppe.
   - **Ressourcen**: Pfade und Namen von Objekten innerhalb des Buckets, für die der Zugriff gewährt oder verweigert wird.

     Die Standardeinstellungen ***bucketname*** und ***bucketname/**** gewähren Zugriff auf alle Objekte im Bucket. Sie können auch Zugriff auf einzelne Objekte gewähren, z. B. ***buchketname/*_readme.txt**.
   - **Bedingungen** (optional): Ausdrücke, die beim Versuch des Zugriffs ausgewertet werden. Sie können beispielsweise eine Liste mit IP-Adressen angeben, für die der Zugriff zulässig oder verweigert wird.

> Ab ONTAP 9.14.1 können Sie Variablen für die Bucket-Richtlinie im Feld **Ressourcen** angeben. Diese Variablen sind Platzhalter, die bei der Bewertung der Richtlinie durch kontextbezogene Werte ersetzt werden. Beispiel: Wenn `${aws:username}` Wird als Variable für eine Richtlinie angegeben, dann wird diese Variable durch den Benutzernamen für den Anforderungskontext ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden.

CLI

Schritte

1. Hinzufügen einer Anweisung zu einer Bucket-Richtlinie:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Die folgenden Parameter definieren Zugriffsberechtigungen:

`-effect`	Die Anweisung kann den Zugriff erlauben oder verweigern
`-action`	Sie können angeben `*` Um alle Aktionen oder eine Liste mit einer oder mehreren der folgenden Aktionen zu bedeuten: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, Und `ListMultipartUploadParts`.

`-principal`	Eine Liste mit einem oder mehreren S3-Benutzern oder -Gruppen. • Es können maximal 10 Benutzer oder Gruppen angegeben werden. • Wenn eine S3-Gruppe angegeben wird, muss sie sich im Formular befinden `group/group_name`. • `*` Kann als öffentlicher Zugriff angegeben werden, d. h. ohne Zugriffsschlüssel und Geheimschlüssel. • Wenn kein Principal angegeben wird, werden allen S3-Benutzern in der Storage-VM Zugriff gewährt.
`-resource`	Den Bucket und jedes darin enthaltene Objekt. Die Platzhalterzeichen `*` Und `?` Kann verwendet werden, um einen regulären Ausdruck zum Angeben einer Ressource zu bilden. Für eine Ressource können Sie Variablen in einer Richtlinie angeben. Bei diesen Richtlinienvariablen handelt es sich um Platzhalter, die bei der Bewertung der Richtlinie durch die Kontextwerte ersetzt werden.

Sie können optional einen Textstring als Kommentar mit dem angeben `-sid` Option.

Beispiele

Im folgenden Beispiel wird eine Bucket-Policy-Anweisung für den Objektspeicher-Server für die Storage-VM svm1.example.com und bucket1 erstellt, die den zulässigen Zugriff auf einen Readme-Ordner für den Objektspeicher-Server-Benutzer Benutzer1 angibt.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

Im folgenden Beispiel wird eine Bucket-Policy-Anweisung für den Objektspeicher-Server für die Storage-VM svm1.example.com und bucket1 erstellt, die den erlaubten Zugriff auf alle Objekte für die Objektspeicher-Servergruppe1 angibt.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

Ab ONTAP 9.14.1 können Sie Variablen für eine Bucket-Richtlinie angeben. Im folgenden Beispiel wird eine Server-Bucket-Richtlinienanweisung für die Storage-VM erstellt `svm1` Und `bucket1`, Und gibt an `${aws:username}` Als Variable für eine Policy-Ressource. Wenn die Richtlinie ausgewertet wird, wird die Richtlinienvariable durch den Benutzernamen für den Anforderungskontext ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden. Wenn beispielsweise die folgende Richtlinienanweisung bewertet wird, `${aws:username}` Wird durch den Benutzer ersetzt, der den S3-Vorgang durchführt. Wenn ein Benutzer `user1` Führt den Vorgang durch, auf den der Benutzer

Zugriff hat `bucket1` Als `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Erstellen oder Ändern einer Objektspeicherserverrichtlinie

Sie können Richtlinien erstellen, die sich auf einen oder mehrere Buckets in einem Objektspeicher anwenden lassen. Serverrichtlinien für Objektspeicher können an Gruppen von Benutzern angehängt werden, wodurch das Management des Datenzugriffs über mehrere Buckets hinweg vereinfacht wird.

Bevor Sie beginnen

Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits vorhanden sein.

Über diese Aufgabe

Sie können die Zugriffsrichtlinien auf der SVM-Ebene aktivieren, indem Sie eine standardmäßige oder benutzerdefinierte Richtlinie in einer Objekt-Storage-Servergruppe angeben. Die Richtlinien werden erst wirksam, wenn sie in der Gruppendefinition angegeben sind.

> Wenn Sie die Objekt-Storage-Server-Richtlinien verwenden, geben Sie Principals (d. h. Benutzer und Gruppen) in der Gruppendefinition und nicht in der Richtlinie selbst an.

Es gibt drei schreibgeschützte Standardrichtlinien für den Zugriff auf ONTAP S3-Ressourcen:

- Vollzugriff
- NoS3Access
- ReadOnlyAccess

Sie können auch neue benutzerdefinierte Richtlinien erstellen, neue Anweisungen für neue Benutzer und Gruppen hinzufügen oder die Attribute vorhandener Anweisungen ändern. Weitere Optionen finden Sie im `vserver object-store-server policy` "Befehlsreferenz".

Ab ONTAP 9.9 unterstützen Sie die Objekt-Tagging-Funktionen von AWS für Clients mit dem ONTAP S3-Server `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging` Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager zum Erstellen oder Ändern einer Objektspeicherserverrichtlinie

Schritte

1. Bearbeiten Sie den Speicher-VM: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf Unter S3.
2. Fügen Sie einen Benutzer hinzu: Klicken Sie auf **Richtlinien** und dann auf **Hinzufügen**.
   a. Geben Sie einen Richtliniennamen ein, und wählen Sie ihn aus einer Gruppenliste aus.
   b. Wählen Sie eine vorhandene Standardrichtlinie aus, oder fügen Sie eine neue hinzu.

      Beim Hinzufügen oder Ändern einer Gruppenrichtlinie können Sie die folgenden Parameter angeben:

      - Gruppe: Die Gruppen, denen der Zugriff gewährt wird.
      - Effekt: Ermöglicht oder verweigert den Zugriff auf eine oder mehrere Gruppen.
      - Aktionen: Zulässige Aktionen in einem oder mehreren Buckets für eine bestimmte Gruppe.
      - Ressourcen: Pfade und Namen von Objekten innerhalb eines oder mehrerer Buckets, für die der Zugriff gewährt oder verweigert wird. Beispiel:
        - * Gewährt Zugriff auf alle Buckets in der Storage-VM.
        - **Bucketname** und **bucketname/*** gewähren Zugang zu allen Objekten in einem bestimmten Bucket.
        - **Bucketname/readme.txt** gewährt Zugriff auf ein Objekt in einem bestimmten Bucket.
   c. Fügen Sie gegebenenfalls Anweisungen zu bestehenden Richtlinien hinzu.

CLI

Verwenden Sie die CLI, um eine Objekt-Store-Serverrichtlinie zu erstellen oder zu ändern

Schritte

1. Objekt-Storage-Server-Richtlinie erstellen:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Erstellen einer Anweisung für die Richtlinie:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Die folgenden Parameter definieren Zugriffsberechtigungen:

`-effect`	Die Anweisung kann den Zugriff erlauben oder verweigern

`-action`	Sie können angeben `*` Um alle Aktionen oder eine Liste mit einer oder mehreren der folgenden Aktionen zu bedeuten: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, Und `ListMultipartUploadParts`.
`-resource`	Den Bucket und jedes darin enthaltene Objekt. Die Platzhalterzeichen `*` Und `?` Kann verwendet werden, um einen regulären Ausdruck zum Angeben einer Ressource zu bilden.

Sie können optional einen Textstring als Kommentar mit dem angeben `-sid` Option.

Standardmäßig werden am Ende der Liste der Anweisungen neue Anweisungen hinzugefügt, die in der Reihenfolge bearbeitet werden. Wenn Sie später Aussagen hinzufügen oder ändern, haben Sie die Möglichkeit, die Anweisungen zu ändern `-index` Einstellung zum Ändern der Verarbeitungsreihenfolge.

Konfigurieren Sie den S3-Zugriff für externe Verzeichnisdienste

Ab ONTAP 9.14.1 sind Services für externe Verzeichnisse in ONTAP S3 Objekt-Storage integriert. Diese Integration vereinfacht die Benutzer- und Zugriffsverwaltung durch externe Verzeichnisdienste.

Sie können Benutzergruppen, die zu einem externen Verzeichnisdienst gehören, mit Zugriff auf Ihre ONTAP Objekt-Storage-Umgebung versehen. Lightweight Directory Access Protocol (LDAP) ist eine Schnittstelle zur Kommunikation mit Verzeichnisdiensten wie Active Directory, die eine Datenbank und Dienste für Identitäts- und Zugriffsmanagement (IAM) bereitstellen. Für den Zugriff müssen Sie LDAP-Gruppen in Ihrer ONTAP S3-Umgebung konfigurieren. Nachdem Sie den Zugriff konfiguriert haben, haben die Gruppenmitglieder Berechtigungen für ONTAP S3 Buckets. Informationen zu LDAP finden Sie unter "Überblick über die Verwendung von LDAP".

Sie können auch Active Directory-Benutzergruppen für den schnellen Bindungsmodus konfigurieren, sodass die Anmeldeinformationen von Benutzern validiert und S3-Anwendungen von Drittanbietern und Open-Source-Anwendungen über LDAP-Verbindungen authentifiziert werden können.

Bevor Sie beginnen

Stellen Sie vor der Konfiguration von LDAP-Gruppen und der Aktivierung des fast-Bind-Modus für den Gruppenzugriff Folgendes sicher:

1. Es wurde eine S3-fähige Storage-VM erstellt, die einen S3-Server enthält. Siehe "Erstellung einer SVM für S3".
2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Erstellen eines Buckets".
3. DNS ist auf der Storage-VM konfiguriert. Siehe "Konfigurieren Sie DNS-Dienste".
4. Auf der Storage-VM wird ein selbstsigniertes CA-Zertifikat (Root Certification Authority) des LDAP-Servers

installiert. Siehe "Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM".

5. Ein LDAP-Client wird mit TLS auf der SVM konfiguriert. Siehe "Erstellen Sie eine LDAP-Client-Konfiguration" Und "Verknüpfen Sie die LDAP-Client-Konfiguration mit SVMs, um Informationen zu erhalten".

Konfigurieren Sie den S3-Zugriff für externe Verzeichnisdienste

1. Geben Sie LDAP als *Name Service-Datenbank* der SVM für die Gruppe und Passwort für LDAP an:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Weitere Informationen zu diesem Befehl finden Sie im "vserver Services Name-Service ns-Switch modify" Befehl.

2. Erstellen einer Bucket-Richtlinienanweisung für Objektspeicher mit dem `principal` Legen Sie die LDAP-Gruppe fest, der Sie Zugriff gewähren möchten:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Beispiel: Im folgenden Beispiel wird eine Bucket-Policy-Anweisung für erstellt `buck1`. Die Richtlinie ermöglicht den Zugriff auf die LDAP-Gruppe `group1` Für die Ressource (Bucket und deren Objekte) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Überprüfen Sie, ob ein Benutzer aus der LDAP-Gruppe stammt `group1` Kann S3-Vorgänge vom S3-Client ausführen.

Verwenden Sie für die Authentifizierung den LDAP-F.A.S.T. Bind-Modus

1. Geben Sie LDAP als *Name Service-Datenbank* der SVM für die Gruppe und Passwort für LDAP an:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Weitere Informationen zu diesem Befehl finden Sie im "vserver Services Name-Service ns-Switch modify" Befehl.

2. Stellen Sie sicher, dass für einen LDAP-Benutzer, der auf den S3-Bucket zugreift, in den Bucket-Richtlinien definierte Berechtigungen gelten. Weitere Informationen finden Sie unter "Ändern einer Bucket-Richtlinie".
3. Überprüfen Sie, ob ein Benutzer aus der LDAP-Gruppe die folgenden Vorgänge ausführen kann:
   a. Konfigurieren Sie den Zugriffsschlüssel auf dem S3-Client in folgendem Format:
   `"NTAPFASTBIND" + base64-encode(user-name:password)`
   Beispiel: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), was dazu führt
   `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

   > Der S3-Client fordert möglicherweise einen geheimen Schlüssel an. In Ermangelung eines geheimen Schlüssels kann ein Passwort mit mindestens 16 Zeichen eingegeben werden.

   b. Führen Sie grundlegende S3-Vorgänge über den S3-Client durch, für den der Benutzer Berechtigungen besitzt.

Ermöglichen Sie LDAP- oder Domänenbenutzern, eigene S3-Zugriffsschlüssel zu generieren

Ab ONTAP 9.14.1 können Sie als ONTAP-Administrator benutzerdefinierte Rollen erstellen und sie lokalen oder Domänengruppen oder LDAP-Gruppen (Lightweight Directory Access Protocol) zuweisen, sodass die Benutzer dieser Gruppen ihren eigenen Zugriff und geheime Schlüssel für den S3-Clientzugriff generieren können.

Sie müssen für Ihre Storage-VM ein paar Konfigurationsschritte durchführen, um die benutzerdefinierte Rolle zu erstellen und dem Benutzer zuzuweisen, der die API zur Schlüsselgenerierung nach dem Zugriff aufruft.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

1. Es wurde eine S3-fähige Storage-VM erstellt, die einen S3-Server enthält. Siehe "Erstellung einer SVM für S3".
2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Erstellen eines Buckets".
3. DNS ist auf der Storage-VM konfiguriert. Siehe "Konfigurieren Sie DNS-Dienste".
4. Auf der Storage-VM wird ein selbstsigniertes CA-Zertifikat (Root Certification Authority) des LDAP-Servers installiert. Siehe "Installieren Sie das selbstsignierte Root-CA-Zertifikat auf der SVM".
5. Ein LDAP-Client wird auf der Storage-VM mit aktiviertem TLS konfiguriert. Siehe "Erstellen Sie eine LDAP-Client-Konfiguration" Und .
6. Verknüpfen Sie die Client-Konfiguration mit dem Vserver. Siehe "Zuordnen der LDAP-Client-Konfiguration zu SVMs" Und "vserver Services Name-Service ldap-Erstellung".

7. Wenn Sie eine Storage-VM verwenden, erstellen Sie eine Management-Netzwerkschnittstelle (LIF) und auf der VM, und außerdem eine Service-Richtlinie für die LIF. Siehe "Netzwerkschnittstelle erstellen" Und "Erstellen der Service-Policy für die Netzwerkschnittstelle" Befehle.

Konfigurieren Sie Benutzer für die Generierung des Zugriffsschlüssels

1. Geben Sie LDAP als *Name Service Database* der Speicher-VM für die Gruppe und Passwort für LDAP an:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Weitere Informationen zu diesem Befehl finden Sie im "vserver Services Name-Service ns-Switch modify" Befehl.

2. Benutzerdefinierte Rolle mit Zugriff auf den REST-API-Endpunkt des S3-Benutzers erstellen:
   `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
   In diesem Beispiel ist der `s3-role` Die Rolle wird für Benutzer auf der Storage-VM generiert `svm-1`, Auf die alle Zugriffsrechte, Lesen, Erstellen und Aktualisieren gewährt werden.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

   Weitere Informationen zu diesem Befehl finden Sie im "Erstellen der Rest-Rolle für die Sicherheitsanmeldung" Befehl.

3. Erstellen Sie eine LDAP-Benutzergruppe mit dem Befehl für die Sicherheitsanmeldung, und fügen Sie die neue benutzerdefinierte Rolle für den Zugriff auf den REST-API-Endpunkt des S3-Benutzers hinzu. Weitere Informationen zu diesem Befehl finden Sie im "Sicherheits-Login erstellen" Befehl.

```
security login create -user-or-group-name <ldap-group-name> -application
http -authentication-method nsswitch -role <custom-role-name> -is-ns
-switch-group yes
```

   In diesem Beispiel die LDAP-Gruppe `ldap-group-1` Wird in erstellt `svm-1`Und die `benutzerdefinierte Rolle `s3role` Wird hinzugefügt, um auf den API-Endpunkt zuzugreifen, zusammen mit der Aktivierung von LDAP-Zugriff im Modus „Fast BIND“.

```
security login create -user-or-group-name ldap-group-1 -application http
-authentication-method nsswitch -role s3role -is-ns-switch-group yes
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

   Weitere Informationen finden Sie unter "Verwenden Sie LDAP fast bind für die nswitch-Authentifizierung".

Durch das Hinzufügen der benutzerdefinierten Rolle zur Domäne oder LDAP-Gruppe erhalten Benutzer in dieser Gruppe eingeschränkten Zugriff auf die ONTAP `/api/protocols/s3/services/{svm.uuid}/users` endpunkt: Durch Aufruf der API können die Benutzer der Domäne oder LDAP-Gruppe eigene Zugriffs- und geheime Schlüssel für den Zugriff auf den S3-Client generieren. Sie können die Schlüssel nur für sich selbst und nicht für andere Benutzer generieren.

Generieren Sie als S3- oder LDAP-Benutzer eigene Zugriffsschlüssel

Ab ONTAP 9.14.1 können Sie eigene Zugriffs- und geheime Schlüssel für den Zugriff auf S3-Clients generieren, sofern Ihr Administrator Ihnen die Rolle zum Generieren eigener Schlüssel eingeräumt hat. Sie können Schlüssel nur für sich selbst generieren, indem Sie den folgenden ONTAP REST-API-Endpunkt verwenden.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt. Informationen zu den anderen Methoden dieses Endpunkts finden Sie in der Referenz "API-Dokumentation".

HTTP-Methode	Pfad
POST	/API/Protokolle/s3/Services/{svm.uuid}/Benutzer

Beispiel für die Wellung

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Beispiel für eine JSON-Ausgabe


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```


Client-Zugriff auf S3-Objekt-Storage aktivieren

Aktivieren Sie ONTAP S3 Zugriff für Remote FabricPool Tiering

Damit ONTAP S3 als Cloud-Tier (Remote FabricPool Capacity) verwendet werden kann, muss der ONTAP S3-Administrator dem Remote-ONTAP-Cluster-Administrator Informationen über die S3-Serverkonfiguration bereitstellen.

Über diese Aufgabe

Die folgenden S3-Serverinformationen sind erforderlich, um FabricPool Cloud-Tiers zu konfigurieren:

- Servername (FQDN)
- Bucket-Name
- CA-Zertifikat
- Zugriffsschlüssel
- Passwort (geheimer Zugriffsschlüssel)

Darüber hinaus ist die folgende Netzwerkkonfiguration erforderlich:

- Der Hostname des Remote-ONTAP S3-Servers muss im für die Admin-SVM konfigurierten DNS-Server einen Eintrag enthalten, einschließlich des FQDN-Namens des S3-Servers und der IP-Adressen auf seinen

LIFs.

- Intercluster LIFs müssen auf dem lokalen Cluster konfiguriert werden, obwohl Cluster-Peering nicht erforderlich ist.

In der FabricPool Dokumentation finden Sie Informationen zur Konfiguration von ONTAP S3 als Cloud-Tier.

"Managen von Storage-Tiers mit FabricPool"

Aktivieren Sie ONTAP S3-Zugriff für lokales FabricPool Tiering

Damit ONTAP S3 als lokale FabricPool-Kapazitäts-Tier verwendet werden kann, müssen Sie einen Objektspeicher basierend auf dem von Ihnen erstellten Bucket definieren und dann den Objektspeicher an ein Performance-Tier-Aggregat anhängen, um eine FabricPool zu erstellen.

Bevor Sie beginnen

Sie müssen über den ONTAP S3-Servernamen und einen Bucket-Namen verfügen, und der S3-Server muss mithilfe von Cluster-LIFs (mit der erstellt wurden `-vserver Cluster` Parameter).

Über diese Aufgabe

Die Objektspeicher-Konfiguration enthält Informationen zur lokalen Kapazitäts-Tier, einschließlich der S3-Server, Bucket-Namen und Authentifizierungsanforderungen.

Eine einmal erstellte Objekt-Storage-Konfiguration darf keinem anderen Objektspeicher oder Bucket zugeordnet werden. Sie können mehrere Buckets für lokale Tiers erstellen, jedoch nicht mehrere Objektspeichern in einem einzelnen Bucket erstellen.

Für eine lokale Kapazitäts-Tier ist keine FabricPool-Lizenz erforderlich.

Schritte

1. Objektspeicher für die lokale Kapazitäts-Tier erstellen:

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - Der `-container-name` Ist der von Ihnen erstellte S3-Bucket.
   - Der `-access-key` Parameter autorisiert Anfragen an den ONTAP S3-Server.
   - Der `-secret-password` Parameter (Secret Access Key) authentifiziert Anforderungen an den ONTAP S3-Server.
   - Sie können die einstellen `-is-certificate-validation-enabled` Parameter an `false` So deaktivieren Sie die Zertifikatprüfung für ONTAP S3.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Anzeigen und Überprüfen der Konfigurationsinformationen des Objektspeichers:

   `storage aggregate object-store config show`

3. Optional: Um zu sehen, wie viele Daten in einem Volume inaktiv sind, führen Sie die Schritte unter aus "Bestimmen der Menge an Daten in einem Volume, die inaktiv sind, mithilfe der inaktiven Datenberichterstellung".

   Wenn Sie feststellen möchten, wie viele Daten in einem Volume inaktiv sind, können Sie entscheiden, welches Aggregat für lokales FabricPool Tiering verwendet werden soll.

4. Verbinden Sie den Objektspeicher mit einem Aggregat:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Sie können das verwenden `allow-flexgroup` **`true`** Sie können Aggregate hinzufügen, die FlexGroup Volume-Komponenten enthalten.

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. Zeigen Sie die Objektspeicherinformationen an, und überprüfen Sie, ob der angeschlossene Objektspeicher verfügbar ist:

   `storage aggregate object-store show`

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

Aktivieren des Client-Zugriffs über eine S3-Applikation

Damit S3-Client-Applikationen auf den ONTAP S3-Server zugreifen können, muss der ONTAP S3-Administrator Konfigurationsinformationen für den S3-Benutzer bereitstellen.

Bevor Sie beginnen

Die S3-Client-App muss in der Lage sein, sich mithilfe der folgenden AWS-Signaturversionen am ONTAP S3-Server zu authentifizieren:

- Signaturversion 4, ONTAP 9.8 und höher
- Signatur Version 2, ONTAP 9.11.1 und höher

Andere Signaturversionen werden von ONTAP S3 nicht unterstützt.

Der ONTAP S3 Administrator muss S3 Benutzer erstellt und ihnen Zugriffsberechtigungen als einzelne

Benutzer oder als Gruppenmitglied, in der Bucket-Richtlinie oder der Objekt-Storage-Server-Richtlinie gewährt haben.

Die S3-Client-App muss in der Lage sein, den ONTAP S3-Servernamen zu beheben. Dazu muss der ONTAP S3-Administrator den S3-Servernamen (FQDN) und die IP-Adressen für die LIFs des S3-Servers angeben.

Über diese Aufgabe

Um auf einen ONTAP S3-Bucket zuzugreifen, geben Benutzer in der S3-Client-Applikation Informationen ein, die der ONTAP S3-Administrator zur Verfügung stellt.

Ab ONTAP 9.9 unterstützt der ONTAP S3 Server die folgenden AWS-Client-Funktionen:

- Benutzerdefinierte Objekt-Metadaten

  Ein Satz von Schlüsselwert-Paaren kann Objekten als Metadaten zugewiesen werden, wenn sie mit PUT (oder POST) erstellt werden. Wenn ein GET/HEAD-Vorgang am Objekt ausgeführt wird, werden die benutzerdefinierten Metadaten zusammen mit den Systemmetadaten zurückgegeben.

- Objekt-Tagging

  Ein separater Satz von Schlüsselwert-Paaren kann als Tags für die Kategorisierung von Objekten zugewiesen werden. Im Gegensatz zu Metadaten werden Tags unabhängig vom Objekt mit REST-APIs erstellt und gelesen. Sie werden auch dann implementiert, wenn Objekte erstellt oder zu einem beliebigen Zeitpunkt danach erstellt werden.

> Damit Clients Informationen zum Tagging abrufen und einfügen können, werden die Aktionen durchgeführt `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging` Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

Weitere Informationen finden Sie in der AWS S3-Dokumentation.

Schritte

1. Authentifizieren Sie die S3-Client-App mit dem ONTAP S3-Server, indem Sie den S3-Servernamen und das CA-Zertifikat eingeben.
2. Authentifizieren Sie einen Benutzer in der S3-Client-App, indem Sie die folgenden Informationen eingeben:
   - S3-Servername (FQDN) und Bucket-Name
   - Zugriffsschlüssel und geheimer Schlüssel des Benutzers

Definitionen von Storage-Services

ONTAP umfasst vordefinierte Storage-Services, die den entsprechenden minimalen Performance-Faktoren zugeordnet sind.

Die tatsächliche Menge an Storage-Services, die in einem Cluster oder einer SVM verfügbar sind, hängt von der Storage-Art ab, aus der ein Aggregat in der SVM besteht.

Die folgende Tabelle zeigt, wie die minimalen Performance-Faktoren den vordefinierten Storage-Services zugeordnet werden:

Storage-Service	Erwartete IOPS (SLA)	IOPS-Spitzenwerte (SLO)	Minimale Volume-IOPS	Geschätzte Latenz	Werden IOPS erzwungen?
Wert	128 pro TB	512 pro TB	75	17 ms	Bei AFF: Ja Ansonsten: Nein
Performance	2048 pro TB	4096 pro TB	500	2 ms	Ja.
Extrem	6144 pro TB	12288 pro TB	1000	1 ms	Ja.

Die folgende Tabelle definiert das verfügbare Storage-Service-Level für jeden Medien- oder Node-Typ:

Medien oder Node	Verfügbares Storage Service Level
Festplatte	Wert
Festplatte einer virtuellen Maschine	Wert
FlexArray-LUN	Wert
Hybrid	Wert
Flash mit optimierter Kapazität	Wert
Solid State Drive (SSD) - kein All Flash FAS System	Wert
Performance-optimierter Flash – SSD (AFF)	Höchste Leistung, Mehrwert